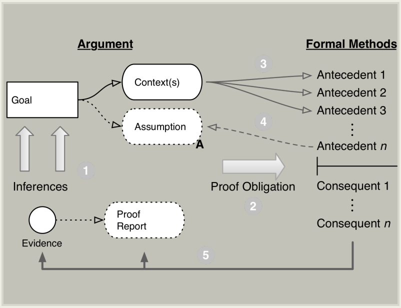
Small Business Innovation Research/Small Business Tech Transfer

Argument-Driven Application of Formal Methods, Phase I

Completed Technology Project (2017 - 2017)

Project Introduction

This proposal, in response to SBIR topic A2.02, develops low-cost, high-assurance UAS autonomy through argument-driven application of formal methods to runtime assurance. Autonomous UAS operations promise lower cost hardware and a reduction in labor force compared to conventionally piloted aircraft. While loss of a UAS may not be catastrophic, the possibility of catastrophic collateral damage exists. UAS software is therefore safety critical, and safety-critical software remains expensive to build and certify. The full economic benefit of autonomous UAS operations cannot be realized until the cost of autonomous UAS software can be reduced without negatively impacting safety. Software architectures providing software fault tolerance through reconfiguration to a trusted backup, such as runtime assurance, offer fixed-cost assurance for autonomous software. They obviate traditional V&V by shifting the assurance burden from the autonomous software to the architecture. Traditional V&V approaches focus on rigorous testing, but providing the level of assurance required to enable UAS autonomy through testing remains infeasible. Formal methods offer an alternative, but comprehensive application of formal methods remains too costly. Application must be targeted at elements of the architecture for which assurance is most critical. Determining where formal methods should be targeted is a challenge. Rigorous safety arguments link safety claims to evidence gathered and not only provide justifiable assurance of safety, but also enable developers and certifiers to identify the most critical elements of the system. Rigorous safety arguments can identify where formal methods should be applied. Argument-driven application of formal methods to runtime assurance therefore provides high assurance of safety while reducing development cost. This circumvents traditional V&V of autonomous UAS software without sacrificing system safety, enabling low-cost high-assurance UAS autonomy.

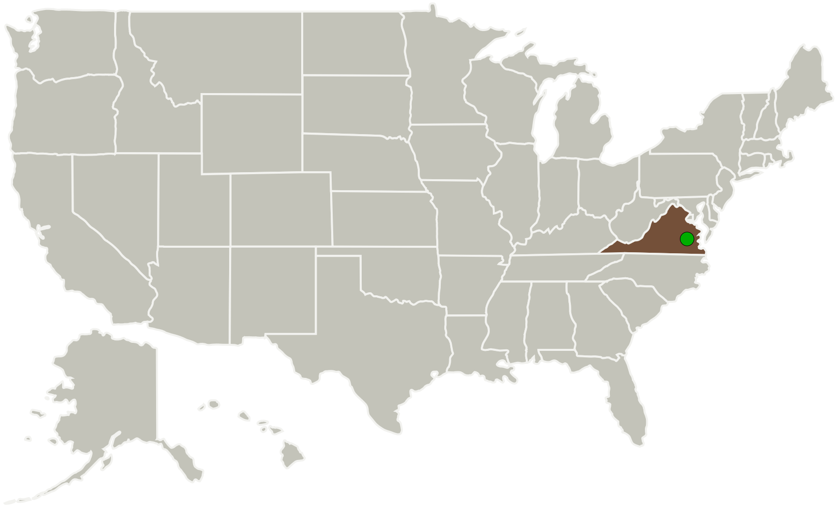


Argument-Driven Application of Formal Methods, Phase I Briefing Chart Image

Table of Contents

Project Introduction 1
Primary U.S. Work Locations and Key Partners 2
Organizational Responsibility 2
Project Management 2
Technology Maturity (TRL) 2
Images 3
Technology Areas 3
Target Destinations 3

Primary U.S. Work Locations and Key Partners



Organizations Performing Work	Role	Type	Location
Dependable Computing, LLC	Lead Organization	Industry	Keswick, Virginia
● Langley Research Center(LaRC)	Supporting Organization	NASA Center	Hampton, Virginia

Primary U.S. Work Locations
Virginia

Organizational Responsibility

Responsible Mission Directorate:

Space Technology Mission Directorate (STMD)

Lead Organization:

Dependable Computing, LLC

Responsible Program:

Small Business Innovation Research/Small Business Tech Transfer

Project Management

Program Director:

Jason L Kessler

Program Manager:

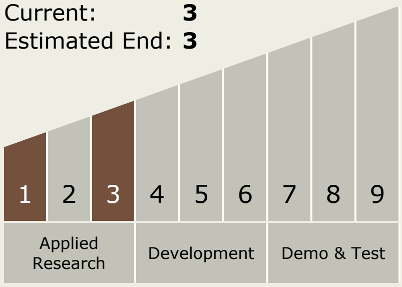
Carlos Torrez

Principal Investigator:

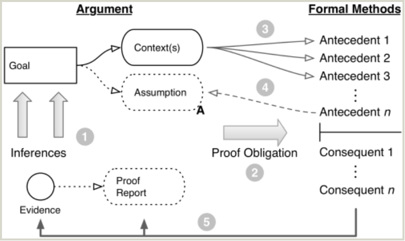
Ashlie B Hocking

Technology Maturity (TRL)

Start:	**1**
Current:	**3**
Estimated End:	**3**



Images



Briefing Chart Image

Argument-Driven Application of Formal Methods, Phase I Briefing Chart Image *(https://techport.nasa.gov/image/128128)*

Technology Areas

Primary:

- TX10 Autonomous Systems
  └ TX10.4 Engineering and Integrity
    └ TX10.4.3 Operational Assurance of Autonomous Systems

Target Destinations

The Moon, Mars, Outside the Solar System, The Sun, Earth, Others Inside the Solar System